Instalacja certyfikatu

Warunkiem poprawnej autoryzacji użytkownika w aplikacji AZU jest zainstalowanie tzw. klucza firmowego w przeglądarce internetowej, wydanego przez NBP w systemie DOCert NBP.

Weryfikacja poprawności oraz ważności certyfikatu klucza firmowego, którego proces instalacji został opisany poniżej, następuje w momencie logowania do AZU. Logowanie zostanie przerwane jeśli użytkownik posłużył się unieważnionym, niepoprawnym lub wygasłym certyfikatem klucza firmowego.

Instalacja certyfikatu klucza firmowego

Do nawiązania bezpiecznego połączenia z aplikacja AZU niezbędne jest posiadanie zainstalowanego w przeglądarce internetowej certyfikatu klucza firmowego wydawanego dla instytucji wydanego w systemie DOCert NBP. Certyfikat taki otrzymuje się w Oddziale NBP na zasadach określonych przez Gestora systemu informatycznego NBP.

Przed rozpoczęciem racy w AZU należy zaimportować certyfikat firmowy instytucji do przeglądarki internetowej, zgodnie z poniższą instrukcją:

Kreator importu klucza firmowego do systemowego magazynu certyfikatów można wywołać z poziomu przeglądarki lub klikając dwukrotnie na plik zawierający klucz firmowy - z rozszerzeniem .p12 lub .pfx

Wywołanie kreatora z poziomu przeglądarki dla:

Chrome (wersja 35): Ustawienia\Pokaż ustawienia zaawansowane\sekcja HTTPS/SSL, przycisk "Zarządzaj certyfikatami".

Instalacja została przestawiona na przykładzie przeglądarki Internet Explorer oraz Mozilla Firefox.

Aby zainstalować certyfikat klucza firmowego w przeglądarce Internet Explorer należy:

- 1. Z menu **Narzędzia** wybrać funkcję **Opcje internetowe**.
- 2. W zakładce **Zawartość** kliknąć przycisk "**Certyfikaty**", a następnie przycisk "**Importuj**".
- 3. Uruchomiony zostanie kreator importu certyfikatów.

Kreator importu certyfikatów		23
	Kreator importu certyfikatów – Zapraszamy! Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów. Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informat używane do ochrony danych lub do ustanawiania bezpie połączeń sieciowych. Magazyn certyfikatów jest obszare systemowym, w którym przechowywane są certyfikaty. Aby kontynuować, kliknij przycisk Dalej.	i cje :cznych em
	< Wstecz Dalej > Anu	luj

4. Należy kliknąć przycisk "Dalej".

5. Wyświetlone zostanie okienko Import pliku, w którym należy wybrać przycisk "**Przeglądaj**".

Kreator importu certyfikatów
Import pliku
Wybierz plik, który chcesz zaimportować.
Nazwa pliku:
Przeglądaj
Uwaga: używając następujących formatów, można przechować więcej niż jeden certyfikat w pojedynczym pliku:
Wymiana informacji osobistych- PKCS #12 (.PFX,.P12)
Standard składni wiadomości kryptograficznych - certyfikaty PKCS #7 (.P7B)
Magazyn certyfikatów seryjnych firmy Microsoft (.SST)
Dowiedz sie wiecei o formatach plików certyfikatów
<pre></pre>

6. Wyświetlone zostanie okienko Otwieranie, w którym należy wskazać położenie certyfikatu otrzymanego w Oddziale NBP (rozszerzenie *.pfx, lub *.p12), a następnie kliknąć przycisk "**Otwórz**".

10 Otwieranie	
G L + Komputer + Dysk lokalny (C) + TEMP +	🔹 😽 🛛 Przeszukoj: TEMP 🖇
Organizuj * Nowy folder	M· 🖬 0
Vilubione Nazwa	Data modyfikacji Typ
 Ostatnie miejsca Pobrane Pulpit 	2016-12-30 10:30 Wymiana Informacji
Biblioteki Dokumenty Muzyka Dorazy Kideo	
A Komputer	
Dysk lokalny (C)	
Nazwa pliku:	m • Wymiana informacji osobisty •
	Otwórz Anuluj

- 7. Kreator powróci do okienka Import pliku, w którym pole **Nazwa pliku** powinno zawierać wskazanie na wybrany certyfikat. Należy nacisnąć przycisk "**Dalej**".
- 8. W okienku **Hasło** należy wprowadzić hasło do klucza prywatnego zawartego w certyfikacie.

Kreator importu certyfikatów	×
Hasło	
W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem.	
Wpisz hasło dla klucza prywatnego.	
Hasto:	
 Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej op użytkownik będzie informowany o każdym użyciu klucza prywatnego pr aplikacje. Oznacz ten klucz jako eksportowalny. Pozwoli to na późniejsze wykona zapasowej lub transport kluczy. 	cji rzez snie kopii
Dołącz wszystkie właściwości rozszerzone	
Dowiedz się więcej o <u>ochronie kluczy prywatnych</u>	
< Wstecz Dalej >	Anuluj

9. Wyświetlone zostanie okienko Magazyn certyfikatów, w którym należy pozostawić wybraną pozycję Automatycznie wybierz magazyn certyfikatów i nacisnąć "**Dalej**".

irych przechowywane są yn certyfikatów; możesz jednak na podstawie typu certyfikatu magazynie Przeglądaj
yn certyfikatów; możesz jednak na podstawie typu certyfikatu magazynie Przeglądaj
na podstawie typu certyfikatu magazynie Przeglądaj
Przeglądaj
Przeglądaj
Przeglądaj

10. W okienku Kończenie pracy Kreatora importu certyfikatów należy wybrać "**Zakończ**".

Kreator importu certyfikatów		×	
	Kończenie pracy Kreatora importu certyfikatów Certyfikat zostanie zaimportowany po kliknięciu przycisku Zakończ. Wybrane zostały następujące ustawienia:		
	Wybrany magazyn certyfikatów Zawartość Nazwa pliku	Automatycznie ustalane PFX C:\Temp\przegl.pfx	
	< Wstecz	Zakończ Anuluj	

Uwaga! Jeżeli wcześniej nie został zainstalowany certyfikat urzędu, zostanie wyświetlone okno dialogowe, w którym należy przede wszystkim sprawdzić nazwę urzędu certyfikacji oraz ewentualnie odcisk palca, następnie dopiero wcisnąć przycisk "Tak".

Pomyślny import certyfikatu klucza firmowego zostanie potwierdzony komunikatem.

Aby zainstalować certyfikat klucza firmowego w przeglądarce Mozilla Firefox należy:

- 1. Z menu Narzędzia wybrać funkcję Opcje.
- 2. W zakładce Zaawansowane wybrać zakładkę Certyfikaty, a następnie przycisk "Wyświetl
- 3. certyfikaty".
- 4. Następnie na formularzu **Menedżera certyfikatów** wybierać zakładkę **Użytkownik**.
- 5. Wybrać przycisk "Importuj".
- 6. Wprowadzić i potwierdzić hasło.

Instalacja zakończona pomyślnie.

Орсје					X	
Ogólne Karty	Treść Aplikacje	Prywatność	Bezpieczeństwo	() Synchronizacja	Zaawansowane	
Ogólne Udostępniar Kiedy serwer żąda © wybierz <u>c</u> ertyfi Wyświ <u>e</u> tl certyfik	nie danych Sieć Aktu osobistego certyfikatu kat automatycznie (aty Weryfikacja Menedżer certyfika Użytkownik Osoby	alizacja Certyfik użytkownika:) py <u>t</u> aj za każdy Urzą <u>d</u> zenia zab utów	raty m razem ezpieczające ny certyfikacji Pozo	ostałe		×
	Posiadasz certyfil Nazwa certyfikat	caty z następując u Urządz	ych organizacji, któ	re cię identyfikują: e Numer si	eryjny Wy	gasa dnia 🛛 🛱
	Wyświetl	<u>K</u> opia zapasowa	K <u>o</u> pia zapaso	wa wszystkich	Importuj	<u>U</u> suń
		oszę podac hasł Wprowadź hasł bezpieczeństwa Hasło:	o o, które będzie użytu tego certyfikatu.	e przy szyfrowaniu OK A	kopii	OK

Po zakończeniu procesu wgrywania certyfikatu należy zamknąć i otworzyć ponownie przeglądarkę, wpisać adres **https://azu.nbp.pl** oraz wprowadzić login i hasło, które mają posłużyć do zalogowania.

Przy pierwszym logowaniu do AZU system wymusi zmianę hasła startowego na unikalne, indywidualne hasło użytkownika systemu ZSZT. Po poprawnym zalogowaniu użytkownik przechodzi do widoku głównego okna aplikacji AZU.

www.nbp.pl